In the Claims

1. (Original) A method for inserting identification or authentication data into digital media data, including the steps of:

segmenting the digital media data into data blocks;

applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block;

applying an orthogonal transform on the modified data block to obtain transform domain data;

modifying at least one selected transform domain data coefficient in accordance with identification or authentication data;

inverse transforming the transform domain data having the at least one modified coefficient; and

applying an inverse pseudo-random function to obtain watermarked digital media data.

2. (Original) A method as claimed in claim 1, wherein the pseudo-random function applied to the data block is a keyed function controlled by a cryptographic key.

3. (Original) A method as claimed in claim 1 or 2, wherein the pseudo-random function applied to the data block has a property of flattening the power spectral density of the data block.

4. (Original) A method as claimed in claim 1, wherein application of the pseudo-random function and application of the orthogonal transform are carried out in the same operation.

5. (Original) A method as claimed in claim 1, wherein the at least one transform domain data coefficient selected for modification is selected according to a keyed pseudo-random operation.

6. (Original) A method as claimed in claim 1, wherein a plurality of data blocks f the digital media data are modified according to the identification or authentication data.

7. (Original) A method as claimed in any one of claims 1 to 6, wherein the digital media data is video data.

8. (Original) A method as claimed in any one of claims 1 to 6, wherein the digital media data is audio data.

9. (Original) A method as claimed in claim 7 or 8, wherein the identification or authentication data is inserted into the digital media data in real time.

10. (Original) A method as claimed in claim 1, wherein at least one coefficient in the transform domain data which represents the average (dc) of the data block is restricted from selection for modification with the identification or authentication data.

11. (Original) A method as claimed in claim 1 or 10, wherein the orthogonal transform is a Walsh Hadamard transform.

12. (Original) A method as claimed in claim 1 or 10, wherein the orthogonal transform is selected from a discrete cosine transform, a discrete sine transform and a fast Fourier transform.

13. (Original) A method as claimed in claim 1, wherein the pseudo-random reversible function is a permutation of the data block based on a keyed pseudo-random number generator.

14. (Original) A method as claimed in claim 1, including determining an average of data values in the data block, subtracting the average value from the data values in the data block before applying the pseudo-random function, and adding the average value

back to the data values in the data block after applying the inverse pseudo-random function.

15. A method for extracting identification or authentication data from watermarked digital media data, including the steps of:

segmenting the digital media data into data blocks;

applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block;

applying an orthogonal transform to the modified data block to obtain transform domain data; and

extracting identification or authentication data from at least one coefficient of the transform domain data.

16. (Original) A method as claimed in claim 15, wherein the pseudo-random function applied to the data block is a keyed function controlled by a cryptographic key.

17. (Original) A method as claimed in claim 15 or 16, wherein the pseudo-random function applied to the data block has a property of flattening the power spectral density of the data block.

18. (Original) A method as claimed in claim 15, wherein application of the pseudo-random function and application of the orthogonal transform as carried out in the same operation.

19. (Original) A method as claimed in claim 15, wherein the extracting step includes selecting at least one transform domain data coefficient from which to extract identification or authentication data according to a keyed pseudo-random operation.

20. (Original) A method as claimed in any one of claims 15 to 19, wherein the digital media data comprises video data.

21. (Original) A method as claimed in any one of claims 15 to 19, wherein the digital media data comprises audio data.

22. A method as claimed in claim 20 or 21, wherein the identification or authentication data is extracted from the digital media data in real time.

23. (Original) A method as claimed in claim 15, wherein the orthogonal transform is a Walsh Hadamard transform.

24. (Original) A method as claimed in claim 15, wherein the orthogonal transform is selected from a discrete cosine transform, a discrete sine transform and a fast Fourier transform.

25. (Original) A method as claimed in claim 15, wherein the pseudo-random reversible function is a permutation of the data block based on a keyed pseudo-random number generator.

26. (Original) A method as claimed in claim 15, including determining an average of data values in the data block, and subtracting the average value from the data values in the data block before applying the pseudo-random function.

27. (Original) An apparatus for inserting or extracting watermark data in digital media data, comprising:

segmenting means for segmenting the digital media data into data blocks;

processing means for applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block and performing a transform on the modified data block to obtain transform domain data; and

means for inserting or extracting watermark data in at least one coefficient of the transform domain data.

28. (Original) An apparatus as claimed in claim 27, wherein the processing means is also adapted to apply an inverse transformation and inverse pseudo-random function of the transform domain data containing the watermark data so as to generate watermarked digital media data.

29. (Original) An apparatus as claimed in claim 27 or 28, wherein the apparatus inserts or extracts watermark data in digital media data in real time.

30. (Original) An apparatus as claimed in claim 29, wherein the digital media data comprises video data.

31. (Original) An apparatus as claimed in claim 29, wherein the digital media data comprises audio data.

32. An apparatus as claimed in claim 27, including means for selecting at least one transform domain data coefficient for the insertion or extraction of identification or authentication data according to a keyed pseudo-random operation.

33. (Original) A media monitoring system comprising:

a media data buffer for temporarily storing media data received from a data source;

a real time processor coupled to receive media data from the media data buffer and adapted to extract identification or authentication data according to the method defined in claim 15; and

a comparison processor coupled to the real time processor for comparing extracted identification or authentication data with known identification or authentication data.

34. (Original) A media monitoring system as claimed in claim 33, including an analogue-to-digital converter for converting media data into a digital form before processing by the real time processor.

35. (Original) A media monitoring system as claimed in claim 33 or 34, wherein the media data comprises video data.

36. (Original) A media monitoring system as claimed in claim 35, wherein the data source of the media data is a receiver of video transmissions.

37. (Original) A media data monitoring method comprising:

receiving media data from a data source;

extracting identification or authentication data according to the method defined in claim 15; and

comparing extracted identification or authentication data with known identification or authentication data.

38. (Original) A media monitoring method as claimed in claim 37, including converting the media data into a digital form before processing by the real time processor.

39. (Original) A media monitoring method as claimed in claim 37 or 38, wherein the media data comprises video data.

40. (Original) A media monitoring method as claimed in claim 39, wherein the media data is received from a video transmission.

41. (New) In a method of steganographically encoding content data to encode a digital watermark therein, the content data representing audio or visual information and comprising plural samples, each having a value, the digital watermark representing a plural-bit payload, the method including segmenting the content data into portions and processing same to encode the digital watermark therein, an improvement comprising subtracting from each of the samples a non-zero value.

42. (New) The method of claim 41 in which the method further includes determining an average value of samples within a portion, and subtracting said average value from each of the samples included in said portion.

43. (New) The method of claim 41 in which the samples in each portion have an order, and the method includes scrambling said order as part of said processing

44. (New) In a method of steganographically encoding content data to encode a digital watermark therein, the content data representing audio or visual information and comprising plural samples, each having a value, the digital watermark representing a plural-bit payload, the method including segmenting the content data into portions and processing same to encode the digital watermark therein, an improvement wherein the samples in each portion have an order, and the method includes scrambling said order as part of said processing.

45. (New) The method of claim 44 that includes scrambling the order of a first portion in a first manner, and scrambling the order of a second portion in a second, different, manner.

46. (New) The method of claim 44 that includes scrambling said order, and thereafter transforming the scrambled data into an orthogonal domain, and thereafter changing the transformed data in accordance with the watermark payload.

47. (New) In a method of steganographically decoding content data to decode a digital watermark therefrom, the content data representing audio or visual information and comprising plural samples, each having a value, the digital watermark representing a plural-bit payload, the method including segmenting the content data into portions and processing same to decode the digital watermark therefrom, an improvement wherein the decoding proceeds without reference to an unencoded original of said content data, and the method includes subtracting from each of the samples a non-zero value.

48. (New) The method of claim 47 in which the method further includes determining an average value of samples within a portion, and subtracting said average value from each of the samples included in said portion.

49. (New) A method of encoding image or video content with a digital watermark comprising:

providing data corresponding to a logo graphic;

providing content data, the content data representing image or video information and comprising plural samples, each having a value;

segmenting the content data into blocks;

transforming the segmented content data into another domain;

processing the transformed content data in accordance with the data corresponding to the logo graphic; and

inverse-transforming the processed content data back into an original domain.

50. (New) In a method of steganographically encoding content data to encode a digital watermark therein, the digital watermark representing a plural bit payload, the content data representing audio or visual information when rendered in a time, or spatial domain, respectively, the method processing said content data in a domain orthogonal to said time or spatial domain, said content data being represented in said orthogonal domain by an array of coefficients, each having a value, an improvement wherein each bit of the watermark payload is associated with at least one of the coefficients, and the method includes assessing a coefficient to determine whether it has an original value consistent with a bit of the watermark payload associated therewith and, if not, then changing the coefficient value, and else leaving the coefficient value unchanged.

51. (New) The method of claim 50 in which a bit of the watermark payload is represented by a sign of a coefficient associated therewith, and the method includes changing the value of the coefficient only if its sign is not in accordance with a value of said watermark payload bit.